DEPARTMENT OF THE NAVY
NAVY MEDICINE EAST
620 JOHN PAUL JONES CIRCLE
PORTSMOUTH, VIRGINIA 23708-2106

NAVMEDEASTINST 3432.1A
M1A
1 Sep 08

NAVMEDEAST INSTRUCTION 3432.1A

Subj: OPERATIONS SECURITY

Ref: (a) OPNAVINST 3432.1

Encl: (1) Command Essential Elements of Friendly Information
(2) Command OPSEC Plan

1. Purpose

a. To provide local guidance in support of reference (a) and to assign responsibilities and direct planning actions to protect the essential secrecy of unclassified, yet critical, mission elements, which may serve as indicators of friendly intentions, Naval capabilities, and current activities to foreign intelligence collection operatives.

b. To publish the Command Operations Security (OPSEC) Plan.

2. Cancellation. NAVMEDEASTINST 3432.1

3. Background. Traditional security programs such as Information Security, Computer Security, Signals Security, Communications Security and Physical Security are primarily designed to protect classified and sensitive but unclassified (SBU) information and material. OPSEC is a non-traditional security program concerned with identifying and protecting generally unclassified information of undertakings. Such indicators may assist those seeking to neutralize or exploit U.S government actions in the area of national security. Reference (a) provides a detailed description of OPSEC doctrine.

4. Scope. The OPSEC program governs all military and civilian personnel assigned to Navy Medicine East (NME). The specific goal for OPSEC at NME is to:

a. Identify those actions that can be observed by hostile intelligence systems.

b. Determine indicators the hostile intelligence system might obtain that could be interpreted or placed together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate, or reduce to an acceptable level, vulnerabilities of friendly actions to hostile exploitation.

5. Policy. This Command will evaluate assigned functions from the OPSEC perspective, identify those of potential interest to adversaries under various circumstances; and determine capabilities and activities that might be conveyed by executing functions. Simple routine activities can involve serious OPSEC weaknesses. Accordingly, OPSEC considerations need to be fully integrated into all daily duties as well as military operations. OPSEC is the responsibility of all hands. As such, the following will be adhered to:

a. Maximum use will be made of the Secure Telephone Unit III (STU III) to discuss unclassified yet sensitive information.

b. Hard copy unclassified but sensitive information will be shredded. This includes information contained within a patient's medical record.

c. Maximum utilization will be made of the Command's Secure Internet Protocol Router Network (SIPRNet) for the communication of classified and sensitive information.

6. Training. Training is a key element of the Command OPSEC Program. Enclosures (1) and (2) will be used for OPSEC training which will be given, at a minimum:

a. To all newly reported personnel who will be trained on local OPSEC threats and procedures within 60 days of reporting.

b. Follow-on training will be conducted annually for all personnel.

7. Responsibilities

a. The Chief of Staff is responsible for ensuring that training, planning, and specific actions are undertaken which enhance the essential secrecy of operational elements, which if otherwise revealed, could deter the effectiveness of the Command, or other units being supported, to accomplish the assigned mission.

b. The Security Manager is responsible for OPSEC planning. He/she will:

(1) Manage the Command's OPSEC Program ensuring full compliance with reference (a);

(2) Conduct OPSEC training as required, but at least annually, for all military and civilian personnel assigned to NME and document this training accordingly;

(3) Identify, in consultation with the Public Affairs Officer (PAO), Essential Elements of Friendly Information (EEFI, enclosure (1) which may be considered for the application of specific OPSEC measures;

(4) Ensure, along with Base Security, the continued viability of other supporting security programs including Information, Personnel, Physical, and Information Systems Security;

(5) Issue an OPSEC report to Chief of Staff when there is a significant change in the Command's OPSEC posture or when a significant vulnerability is identified.

c. The Training Officer will sponsor and monitor accomplishment of training for all staff.

8. Action. This plan is effective upon receipt for planning and operations in support of OPSEC.

PETER F. O'CONNOR
Chief of Staff

Distribution: (NAVMEDEASTINST 5215.1)
List A

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

1. It is essential to be able to identify key adversary questions about friendly intentions and military capabilities to which answers will probably be sought. These questions constitute Essential Elements of Friendly Information (EEFI). Sensitive aspects of our operations therefore require protection. Listed below are indicators that serve as a guide in recognizing EEFI (e.g., they are areas of interest to the enemy, etc.). This list is not all-inclusive.

a. Classified information/sources.

b. Non-classified information/sources dealing with administration, logistics, operations, and communications.

(1) Administration. Unusual types/numbers of TAD orders, rate/rating, advance pay for a large number of personnel and arranging for special support services.

(2) Logistics. Inordinate mail movement or an increased tempo in ordering medical supplies.

(3) Operations. Propositioning supplies or medical personnel, conducting drills, and deviating from normal activity.

(4) Communications. Change in message volume and an increase in the use of the STU III.

c. Details or references to plans or operations.

d. Medical deployments that indicate possible operational intent or activity.

f. Existence or use of special plans.

g. Real world contingency plan in association with an exercise.

h. Prepositioning of equipment and supplies in preparation for operations.

i. Personnel records and information.

j. Movement of VIPs.

k. Open sources of information such as newsletters, press releases, and command publications.

2. The following are common actions that lend to the disclosure of EEFI:

a. Congregating in establishments.

b. Poor access control to operational and administrative areas.

c. Use of unsecured voice transmissions (telephone).

d. Leaving LANs on line when not in use.

e. Unauthorized civilian or military personnel present in workspaces.

COMMAND OPSEC PLAN

1. Purpose. To provide specific planning guidance for implementing an OPSEC program at the Navy Medicine East.

2. Threats. There are various types of threats that face the Command where OPSEC measures may be of value.

a. Theft. Hostile intelligence organizations, disaffected personnel, and criminals observe physical security practices to find vulnerabilities they can exploit to steal documents of value.

b. Personnel Subornment. Hostile intelligence organizations and criminals gather data about personnel to detect access to matters of interest in personnel character, indebtedness, and other vulnerabilities. Thus, the OPSEC practices of individuals, personnel offices, finance offices, and others who deal with personnel records must be such as to keep secret indicators that could be used by adversaries.

c. Terrorism. The Command must ensure Command personnel are aware of and, when a terrorist intent and capability is present, use OPSEC measures to reduce vulnerabilities to attack.

d. Inadvertent Disclosures. The inadvertent introduction of open source indicators by statements, press releases, conversations, articles, letters, and other actions poses an OPSEC threat. Hostile intelligence services train personnel in techniques for eliciting information during conversations, frequenting areas where government employees congregate as well as gathering base newspapers, Plans of the Day, telephone books, organizational manuals, technical manuals and other such data. The Command must ensure that personnel are aware of the questions hostile intelligence may pose to gather specific information and are aware of the potential indicators they must protect.

3. Structure. The Command Security Manager has primary responsibility for implementing the OPSEC program. Other elements having significant OPSEC responsibilities are the Information Systems Security Officer, and Personnel Management staff.

4. Training. For OPSEC to be effective, military, civil service, and contract personnel must understand the concept of OPSEC and apply that knowledge and awareness in the performance of assigned tasks. The Command Security Manager and Training Officer have responsibility for ensuring that OPSEC training is accomplished. The content of the Command's OPSEC training program should be designed to answer the following questions personnel are likely to ask:

(1) "Why is OPSEC important generally and specifically to my organization?"

(2) "Why is OPSEC important to me?" and

(3) "How can I contribute to OPSEC?"

a. Provide OPSEC training to newly reporting personnel within 60 days of reporting to or being hired by the Command.

b. Implement a continuing awareness campaign through annual refresher training in OPSEC and counter terrorism and/or discussion of specific concerns.

c. Provide individuals in key assignments additional OPSEC planning skills preceding and during the execution of sensitive operations or support missions. Consider external resources (i.e., Naval Criminal Investigative Service, Base Security, etc.) to assist in this training.